(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2002 (14.02.2002)

PCT

(10) International Publication Number
WO 02/13436 A1

(51) International Patent Classification[7]: H04K 1/02

(21) International Application Number: PCT/US01/24468

(22) International Filing Date: 2 August 2001 (02.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/634,506 9 August 2000 (09.08.2000) US

(71) Applicant: AVWAY.COM INC. [US/US]; 12 Broad Street, Red Bank, NJ 07701 (US).

(72) Inventors: RAMKUMAR, Mahalingam; Apartment 4A, 55 Belgrove Drive, Kearny, NJ 07032 (US). AKANSU, Ali, N.; 181 Heights Terrace, Middletown, NJ 07032 (US).

(74) Agent: GREELEY, Paul, D.; Ohlandt, Greeley, Ruggiero & Perle, L.L.P., 10th floor, One Landmark Square, Stamford, CT 06901-2682 (US).

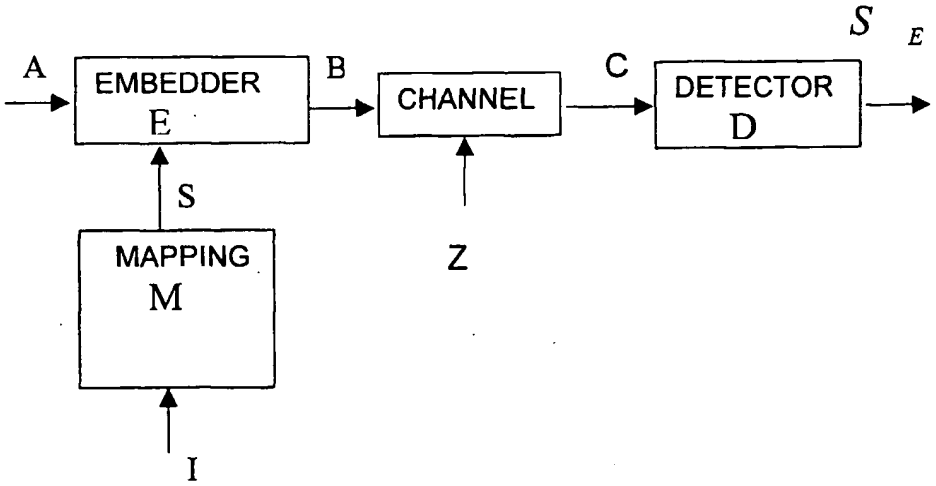
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR STEGANOGRAPHICALLY EMBEDDING INFORMATION BITS IN SOURCE SIGNALS



(57) Abstract: A method and system for embedding (E) information bits in a source signal (A) like images, audio or video. The embedding being performed optimally for a given worst-case scenario of unintentional or intentional attack of the host signal (to remove the embedded bits), and a given distortion of the host signal due to information embedding.

WO 02/13436 A1

METHOD AND SYSTEM FOR STEGANOGRAPHICALLY EMBEDDING INFORMATION BITS IN SOURCE SIGNALS

This invention relates to a method and system for embedding information bits in a host signal. The embedding may be performed to determine origin of any perfect or imperfect copies of the composite (host plus message) signal, or to use the host signal as a cover for secret or covert communications, over a channel which is primarily meant for transmitting the host signal only.

BACKGROUND OF THE INVENTION

Data hiding or steganography is the art of hiding a message signal in a host signal, without any perceptual distortion of the host signal. The composite (host plus message) signal is also referred to as stego-signal. Though steganography is often confused with the relatively well-known cryptography, the two are but loosely related. Cryptography is about hiding the contents of a message. Steganography, on the other hand, is about concealing the very fact that a message is hidden. Steganography may be considered as communication through subliminal channels, or secret communication.

Rapid increases in bandwidth available for dissemination and storage of digital content and availability of software tools for editing multimedia content, such as, video, images or audio calls for systems and methods to establish origin of such content. In addition, large volumes of multimedia content being exchanged over insecure channels, such as, the Internet, provide within themselves secure and subliminal steganographic channels for secure or secret communications.

The proliferation of digital multimedia as opposed to conventional analog forms, is primarily a result of (1) the ease with which digital data can be exchanged over the Internet, and (2) the emergence of efficient multimedia data compression techniques.

The first reason listed above is also a major cause for concern. Unlimited perfect copies of the original content can be made, and distributed easily. It was this concern of protecting intellectual property rights of multimedia data in digital

form, that primarily triggered researchers to find ways to watermark multimedia data. Watermarking the content is done by embedding some data in the host signal (original content). The embedded data may be an imperceptible signature, which the owner of the multimedia content should be able to extract when a dispute regarding ownership occurs.

Data hiding in multimedia could help in providing proof of origin and distribution of content. Multimedia content providers would be able to communicate with the compliant multimedia players (or renderers) through the subliminal, steganographic channel. This communication may control or restrict access of multimedia content, and carry out e-commerce for pay-per-use implementations.

A typical application of data hiding for multimedia content delivery may involve the content providers supplying the raw multimedia data (say a full length movie) along with some hidden agents or control data . The job of the distributors would be to package the content in some suitable format (such as, MPEG) understandable by the player, for distribution of the multimedia through DVDs/CDs or live digital broadcasts, or by hosting web sites for downloads or streaming. The compliant multimedia players, will typically be connected to the Internet.

In conventional multimedia distribution, the content provider looses all control over how the multimedia is used/abused the moment it is acquired by another party. The key idea behind data hiding is to re-establish control whenever the content is used. The content provider, by hiding an agent in his raw data, hopes to control access to his/her multimedia content. This can be done with the co-operation of the players, and an established protocol for communication between the content providers and the compliant multimedia players.

Data hiding can be broadly classified into two categories depending on whether the original content is needed for extraction of the hidden bits: (1) non-oblivious methods need the original content for extracting the hidden bits; and (2)

on the other hand, oblivious detection methods extract the hidden bits without any knowledge of the original.

In most data hiding methods, sequence of bits to be embedded, viz. B, is converted to a form suitable for embedding in a cover content. Initially, the bit sequence is converted to a signature sequence. Thereafter, the signature sequence is embedded in the cover content by an embedding function to obtain the stego-content.

From a signal processing perspective; data hiding methods can be classified into two categories, depending on the type of embedding and detecting operators. The first category includes methods where the embedding function adds the signature sequence linearly to stego-content, and the detector detects from the stego-content via correlative processing (these methods are referred to as Type I methods in data hiding literature). In the second category the embedding function and the detector are non-linear, typically employing quantizers (these methods are referred to as Type II methods in data hiding literature). One of the important characteristics of the non-linear methods is their ability to suppress the noise due to the original content (or self-noise), even though the original content is not available at the receiver.

The present invention provides a unique data hiding technique that substantially reduces the effect that noise, distortion or corruption of the host signal have on the detected signal so as to greatly enhance the integrity of steganography techniques employing oblivious detection of the hidden data. The crux of the invention is a class of methods referred to as Type III methods of which Types I and II are just special cases. An optimal choice of parameters for the proposed Type III methods depending on the engineering constraints, can substantially improve the performance of data hiding.

The present invention also provides many additional advantages, which shall become apparent as described below.

SUMMARY OF THE INVENTION

A method for embedding a message signal in a host signal, the method comprising the steps of:

(a) embedding the message signal into the host signal, thereby producing a stego signal; and

(b) detecting an estimate of the message signal from the stego signal; provided that the detecting step (b) is not an exact inverse of the embedding step (a), and the host signal cannot be exactly extracted from the stego signal.

The embedding step (a) produces a value b_i in the stego signal from a value a_i in the host signal, and wherein the embedding step (a) comprises limiting to a limit value $\frac{\beta}{2}$, a magnitude of difference between b_i and a_i.

Furthermore, the embedding step (a) employs a continuous periodic function to produce the stego signal, and wherein the detecting step (b) employs a continuous periodic function to produce the estimated message signal. The continuous periodic function is a triangular function $f(x)$ having a period Δ, wherein:

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x;}$$

$$f(0) = -\frac{\Delta}{4}; \quad \text{and}$$

$$f(\frac{\Delta}{2}) = \frac{\Delta}{4}$$

Optionally, the embedding step (a) produces a value b_i in the stego signal from a value a_i in the host signal and a value s_i in the message signal, such that the embedding step (a):

(i) is subject to a maximum distortion constraint P,

(ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $b_i = E(a_i, s_i)$, and employs an algorithm as follows:

$$\text{if } rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}, \text{ then } p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta}),$$

$$\text{else } p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4};$$

$$e_i = s_i - p_i;$$

$$\text{if } (|e_i| > \frac{\beta}{2}), \text{ then } e_i = sign(e_i)\frac{\beta}{2};$$

$$q_i = rem(\frac{a_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2}, \text{ then } e_i = -e_i;$$

$$\text{if } a_i > 0, \text{ then } b_i = a_i + e_i,$$

$$\text{else } b_i = a_i - e_i.$$

The method of the present invention is particularly useful when the stego signal is corrupted or distorted prior to detecting step (b). In this embodiment where the stego signal is corrupted a value b_i in the stego signal is modified after the embedding step (a) to yield a value c_i in the corrupted or distorted stego signal, such that the detecting step (b):

(i) produces a value s_{ei} in the estimated message signal from a value c_i in a distorted stego signal,

(ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $s_{ei} = D(c_i)$, and employs an algorithm as follows:

$$q_i = rem(\frac{c_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2}, \text{ then } s_{ei} = 3\frac{\Delta}{4} - q_i,$$

$$\text{else } s_{ei} = q_i - \frac{\Delta}{4}.$$

Preferably the host signal is a sequence a_i, for $i=1$ to N; the message signal is a sequence s_i, for $i=1$ to N; the stego signal is a sequence b_i, for $i=1$ to N; the corrupted or distorted stego signal is a sequence c_i, for $i=1$ to N; and the estimated message signal is a sequence s_{ei}, for $i=1$ to N.

The embedding step (a) preferably (i) imposes a limit $\frac{\beta}{2}$ on a magnitude difference between a value b_i in the stego signal that is produced from a value a_i in the host signal; and (ii) employs a continuous periodic function having a period Δ to produce the stego signal, wherein such the limit $\frac{\beta}{2}$ and the period Δ are chosen to minimize a mean square distance between the message signal and the estimated message signal, subject to a maximum distortion constraint P of the embedding step (a).

The present invention also provides a method for mapping K information bits to a message signal s_i, $i=1$ to N. This method comprising the step of: grouping the K information bits together to represent one of 2^L symbols, wherein each of the 2^L symbol is mapped to a basis vector or its negative of a $2^{L-1} \times 2^{L-1}$ orthogonal transform matrix. The orthogonal transform matrix is obtained from a cyclic all-pass filter and its circular shifts. The cyclic all-pass filter is preferably obtained from a key.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of the data embedding, channel and detection operation according to the present invention;

Fig. 2 is a graph depicting a periodic triangular function employed by the detector D of Fig. 1;

Fig. 3(a) is a graph demonstrating that the distortion introduced during the embedding the S in A (to obtain B) of Fig. 1 in accordance with Type II will be uniformly distributed between $-\frac{\Delta}{2}$ and $+\frac{\Delta}{2}$;

Fig. 3(b) is a graph depicting the distribution of the distortion introduced in accordance with the method of the present invention; and

Fig. 3(c) is a graph depicting the distribution of the limiting noise t_i.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a method for efficient secure communication over subliminal channels provided by multimedia host signals like audio, images and video transmitted over any channel. For example, the host signal may be transmitted over the Internet or distributed in storage mediums by other means or even transmitted over analog channels, such as, that used for analog television or radio broadcasts. Typically the host signal is expected to undergo some distortion before it reaches one or many end points where it may be stored or rendered.

In the method described herein, the host signal may be any form of naturally occurring signals, such as, audio, image or video or artificially synthesized versions of them. The host signal may further be represented in some transform domain. The choice of the transform may depend on the nature of the application. For example, if the host signal is an image and is not expected to be re-scaled, resized or rotated, any unitary transform may be used. On the other hand, if the image is likely to undergo rotation, scaling and/or translation, a Rotation-Scale-Translation invariant transform may be used. If the image is cropped, data embedding may be performed in many blocks of the image, so that the hidden bits can be extracted even if one such block survives. In general, the host signal can be coefficients of a one-to-one transform or a many-to-one transform.

In the method described herein, the host signal can therefore be considered as a vector or a sequence of N real or complex numbers, represented by

$$A = [a_1 \quad a_2 \quad \cdots \quad a_N].$$

A sequence of K bits, represented by

$$I = [i_1 \quad i_2 \quad \cdots \quad i_K], \; i,j = 1/0 \text{ for } 1 \le j \le K$$

is mapped by a mapping M to a signature sequence S,

$$M : I \rightarrow S, \text{ where}$$

$$S = [s_1 \quad s_2 \quad \cdots \quad s_N]$$

An embedder E embeds the sequence in A to obtain the stego sequence B, $B = E(A,S)$, where

$$B = [b_1 \quad b_2 \quad \cdots \quad b_N],$$

the embedding being performed element-wise,

$$\begin{aligned} b_1 &= E(a_1, s_1) \\ b_2 &= E(a_2, s_2) \\ b_3 &= E(a_3, s_3) \\ &\vdots \\ b_N &= E(a_N, s_N) \end{aligned}$$

subject to the constraint that $d(A,B) \le P$ where $d(A,B)$ is some distance measure of signals A and B, and P is the maximum permitted distortion of the host signal. In the preferred embodiment the distance measure is the mean square error:

$$d(A,B) = \frac{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots + (a_N - b_N)^2}{N}$$

The stego sequence B may undergo some distortion before it reaches the detector as C, given by $C = B + Z$, where

$$Z = [z_1 \quad z_2 \quad \cdots \quad z_N],$$

is the noise in the channel used for transmitting the host signal, and

$$C = [c_1 \quad c_2 \quad \cdots \quad c_N].$$

The detector D obtains an estimate S_e of the signature sequence S embedded:

$$S_e = D(C).$$

The block diagram of data embedding, the channel and detection operation is shown in FIGURE 1.

Based on this generalization of the embedding and detecting functions E and D, prior art in this field can be categorized into two types.

Characteristics of Type I

- $B = E(A,S) \rightarrow B = A + S$
- $D(B) = A + S \neq S$

The above two equations imply that E and D are not inverses. In addition, if S is known one can obtain the original host sequence A from B as $A = B - S$.

Characteristics of Type II

- $B = E(A,S)$
- $D(B) = S$

Unlike Type I methods, the above two equations show that for Type II methods E and D are exact inverses. Additionally, unlike Type I methods, it is not possible to obtain A exactly, given B and S.

In the core of this invention is a class of embedding and detection operators E and D, we shall refer to as Type III.

Characteristics of Type III

- $B = E(A,S)$
- $D(B) \neq S$

The above two equations illustrate that E and D are not exact inverses (like Type I and unlike Type II). Further, given S and B it is not possible to obtain A (like Type II and unlike Type I).

In a preferred embodiment described herein, the detector D, where

$$S_e = D(C),\ S_e = [s_{e1} \quad s_{e2} \quad \cdots \quad s_{eN}]$$

is implemented by the following algorithm:

$$q_i = rem(\frac{c_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2} \text{ then } s_{ei} = 3\frac{\Delta}{4} - q_i,$$

$$\text{else } s_{ei} = q_i - \frac{\Delta}{4}.$$

In the above algorithm, rem (x) stands for the remainder of a division operation (x). For example,

rem(5/4)=1, rem(2/2)=0, rem(-6/4)=rem(6/4)=2.

The choice of the parameter Δ is dictated by the distortion constraint P and the energy of the channel noise Z. The detector may also be thought of as employing a periodic triangular function shown in FIGURE 2,

$$y = f(x) = f(x + m\Delta) \text{ for integer } m. \text{ Also,}$$

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x,}$$

and specifically,

$$f(0) = -\frac{\Delta}{4}$$

$$f(\frac{\Delta}{2}) = \frac{\Delta}{4}$$

The embedding operation $b_i = E(a_i, s_i)$ is implemented by the following algorithm:

$$\text{if } rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}, \text{ then } p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta}),$$

else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$;

$e_i = s_i - p_i$;

if $(|e_i| > \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$;

if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $e_i = -e_i$;

if $a_i > 0$, then $b_i = a_i + e_i$,

else $b_i = a_i - e_i$.

In the above algorithm, β is a parameter, the choice of which is dictated by the distortion constraint P and the energy of the channel noise Z. Also sign (x) equals +1 if the quantity 'x' is positive and sign (x) equals –1 if the quantity 'x' is negative. For example,

sign(-20) = sign(-1) = -1, and sign(11) = sign(1) = +1.

As an example of the embedding and detection operations, let

A=[-65, –250, 19, 43, –172, 179, 178, –6], and

S=[10, 10, –10, 10, –10, 10, –10, 10],

$\Delta = 40$, and $\beta = 10$ (Note that $-\frac{\Delta}{4} \le s_i \le \frac{\Delta}{4}$ for all i).

Now $B = E(A,S)$ is given by

B=[-60, –255, 14, 48, –167, 180, 173, –11]. Let

Z=[-4, –8, 2, –10, –5, 3, –6, -4]. Therefore,

C=B+Z=[-64, –263, 16, 38, –172, 183, 167, –15], and

$S_e = D(C)$ is now

S_e = [6, 7, 6, –8, 2, 7, –3, 5].

Now let us consider $b_i = E(a_i, s_i)$, for i=1. $a_1 = -65$, $s_1 = 10$.

If $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta})$,

$rem(\frac{-65}{40}) = 25 \ge \frac{\Delta}{2}$, $p_1 = 30 - 25 = 5$

else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$

$e_i = s_i - p_i$ $e_1 = 10 - 5 = 5$

if $(|e_i| > \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$ $e_1 = \frac{\beta}{2}$

if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$ $e_i = -e_i$ $rem(\frac{-65}{40}) = 25 > \frac{\Delta}{2}$, $e_1 = -5$

if $a_i > 0$ $b_i = a_i + e_i$

else $b_i = a_i - e_i$ $b_1 = -65 - (-5) = -60$

Now $c_1 = b_1 + z_1 = -60 - 4 = -64$. For detection,

$q_i = rem(\frac{c_i}{\Delta})$. $q_1 = rem(\frac{-64}{40}) = 24$

if $q_i > \frac{\Delta}{2}$ then $s_{ei} = 3\frac{\Delta}{4} - q_i$ $q_1 = 24 > 20$, $s_{e1} = 30 - 24 = 6$

else $s_{ei} = q_i - \frac{\Delta}{4}$

For Type II systems ($\Delta = \beta$) the distortion introduced, viz. $B - A$ for embedding the S in A (to obtain B) will be uniformly distributed between $-\frac{\Delta}{2}$ and $+\frac{\Delta}{2}$ (FIGURE 3a), and the average energy of the distortion introduced in A will be $\frac{\Delta^2}{12}$. For Type III systems, the distribution of the distortion introduced is depicted in FIG. 3b. The average energy of the distortion for a Type III system is given by

$$\frac{\beta^2(3\Delta - 2\beta)}{12\Delta}.$$

While for Type II systems $s_i = D(b_i)$, for the proposed Type III system

$D(b_i) - s_i = t_i$

where t_l is noise due to "limiting" (limiting occurs when $\beta < \Delta$). The distribution of the limiting noise t_l is shown in FIG. 3c, and the average energy of the limiting noise is given by

$$\frac{(\Delta-\beta)^3}{12\Delta}.$$

Optimal choice of the parameters Δ and β for a given signal-to-noise ratio (snr)

$$\text{snr} = \frac{\text{Signal Energy}}{\text{Noise Energy}} = \frac{P = \frac{\beta^2(3\Delta-2\beta)}{12\Delta}}{\text{Energy of Channel Noise } Z}$$

is shown in Table 1. In Table 1,

$$\text{SNR} = 10\log_{10}(\text{snr})\ \text{dB}, \text{ and}$$

$$k = \frac{\Delta}{\sqrt{\frac{P}{12}}}$$

From the values of Δ and signal energy P, β can be obtained by solving

$$\frac{\beta^2(3\Delta-2\beta)}{12\Delta} = P$$

Table 1 – Optimal Choice of k for different SNRs

SNR	k
4.77	1.24
3.01	1.40
1.76	1.55
0.00	1.87
-3.01	2.57
-4.77	3.14
-6.02	3.59
-6.99	4.04
-7.78	4.40
-8.45	4.78

-9.03	5.11
-9.54	5.41
-10.00	5.71
-13.01	8.10
-14.77	9.95

The optimal parameters are chosen to minimize

$$J = \frac{(s_1 - s_{e_1})^2 + (s_2 - s_{e_2})^2 + \cdots + (s_N - s_{e_N})^2}{\Delta^2},$$

which is the normalized mean square distance between the embedded signature sequence and the detected signature sequence. The minimization performed under the assumption that the channel noise Z has a Gaussian distribution. If Z is zero mean and has a variance of σ_z^2, then

$$J = \frac{1}{\Delta^2}\sum_{i=0}^{\infty}\int_{\frac{\Delta}{2}}^{\frac{(i+1)\Delta}{2}}\left(\frac{(2i+1)\Delta}{4} - z\right)^2 f_Z(z)\mathrm{d}z,$$

where

$$f_Z(z) = \frac{\beta}{2\sqrt{2\pi\sigma_z^2}}\mathrm{e}^{-\frac{z^2}{2\sigma_z^2}} + \frac{1}{2\Delta}\left\{\mathrm{erf}\left(\frac{z+\frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_z}\right) - \mathrm{erf}\left(\frac{z-\frac{\Delta-\beta}{2}}{\sqrt{2}\sigma_z}\right)\right\},$$

and

$$\mathrm{erf}(t) = \frac{2}{\pi}\int_0^t \mathrm{e}^{-\frac{y^2}{2}}\mathrm{d}y$$

The mapping

$$M : I \to S,$$

in the preferred embodiment takes the following form. The bit sequence I of K bits is grouped into K/L L-bit symbols. Each L-bit symbol will be mapped to one of in 2^{L-1} basis vectors of an orthogonal transform. Thus we can embed $\frac{N}{2^{L-1}}$ symbols or $\frac{NL}{2^{L-1}}$ bits in the sequence A. For example,

if N=8192, for

L = 2, 3, 4, 5, 6, 7, 8, 9, and 10,

K = 8192, 6144, 4096, 2560, 1536, 896, 512, 288, and 160 bits respectively.

In the preferred embodiment, L bits corresponding to each symbol are assumed to represent a decimal number between 1 and 2^{L-1}. This number is used as the index of the basis vector to be chosen.

The basis vectors of a $Q \times Q$ orthogonal transform where $Q = 2^{L-1}$ are obtained from a random seed as follows. The random seed (or key) is used to generate uniformly distributed random sequence

$$[\theta_1, \ \theta_2, \ \cdots \ , \theta_{(\frac{Q}{2}-1)}], \ -\pi \le \theta_i \le \pi .$$

The $\frac{Q}{2}-1$ random numbers define the phase of the discrete Fourier transform (DFT) of a sequence H. The magnitudes of the discrete Fourier coefficients are assumed to be unity. Such a sequence H is cyclic all-pass of length Q. H is orthogonal to all its cyclic shifts. Such a sequence derived from a random seed and all its cyclic shifts form a complete basis, and can therefore be considered as the basis vectors of a $Q \times Q$ unitary transform matrix.

As an example, let Q=8. Let the $\frac{Q}{2}-1$=3 random numbers be

[-2.7489, –0.7854, 1.1781].

These random numbers describe are the angles of the Discrete Fourier Transform coefficients of H. The angles of the 8 coefficients of H are

[0, –2.7489, –0.7854, 1.1781, 0, –1.1781, 0.7584, 2.7489]

and their magnitudes are equal to 1. The cyclic all-pass filter H is obtained by inverse Discrete Fourier Transform as

[0.2915, –0.1499, 0.3999, –0.0415, 0.5621, 0.5034, –0.2534, –0.3121]

Each segment of length Q of the signature sequence S of length N carries information pertaining to one symbol between 0 and 2Q-1.

Symbol sequence - $[y_1, \ y_2, \ \cdots \ , y_{\frac{N}{Q}}]$; $0 \le y_i \le 2Q-1$ for all i

Signature sequence - $[S_1, \ S_2, \ \cdots \ , S_{\frac{N}{Q}}] = S$

The algorithm for obtaining the signature sequence is as follows

for all i

sign=1;

if $y_i \ge Q$

shift = $y_i - Q$;

sign = -1;

else

shift = y_i;

circularshift (sign x H, shift);

For example, if

H = [0.2915, –0.1499, 0.3999, –0.0415, 0.5621, 0.5034, –0.2534, –0.3121] and $y_i = 2$ (circular shift by 2) then,

S_i = [-0.2534, –0.3121, 0.2915, –0.1499, 0.3999, -0.0415, 0.5621, 0.5034].

As an other example, if y_i = 10 (circular shift by 10-8=2 followed by negation), then

S_i = [0.2534, 0.3121, -0.2915, 0.1499, -0.3999, 0.0415, -0.5621, -0.5034].

The Algorithm for the inverse mapping $M^{-1} : S_e \rightarrow I_e$ is as follows:

Each segment of length Q of the detected sequence $S_e = [S_{e1}, \ S_{e2}, \ \cdots \ , S_{e\frac{N}{Q}}]$ corresponds to a symbol. The embedded symbol is estimated as follows:

HH=DFT(H)

for all i

SS=DFT(S_{ei});

YY=IDFT(SS.*HH);

y_{ei}=index(max(abs(YY)));

if (YY[y_{ei}]) < 0, then

$y_{ei}=y_{ei}$+Q

In the above algorithm, DFT stands for Discrete Fourier Transform and IDFT stands for Inverse DFT. y_{ei} is the estimate of y_i, which is the symbol embedded in the i'th segment of S. Finally, the binary representation of e y_{ei} yields the corresponding sequence of bits I_{ei}, and

$$I_e = [I_{e1}, \quad I_{e2}, \quad \cdots \quad , I_{e\frac{N}{Q}}].$$

I_e is the estimate of the hidden bit sequence I.

WHAT IS CLAIMED IS:

1. A method for embedding a message signal in a host signal, said method comprising the steps of:
   (a) embedding said message signal into said host signal, thereby producing a stego signal; and
   (b) detecting an estimate of said message signal from said stego signal; provided that said detecting step (b) is not an exact inverse of said embedding step (a), and said host signal cannot be exactly extracted from said stego signal.

2. The method according to claim 1, wherein said stego signal is corrupted or distorted prior to detecting step (b).

3. The method according to claim 1, wherein said embedding step (a) produces a value b_i in said stego signal from a value a_i in said host signal, and wherein said embedding step (a) comprises limiting to a limit value $\frac{\beta}{2}$, a magnitude of difference between b_i and a_i.

4. The method according to claim 1, wherein said embedding step (a) employs a continuous periodic function to produce said stego signal, and wherein said detecting step (b) employs said continuous periodic function to produce said estimated message signal.

5. The method according to claim 4, wherein said continuous periodic function is a triangular function.

6. The method according to claim 5, wherein said triangular function $f(x)$ has a period Δ, and
   wherein:

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x;}$$

$$f(0) = -\frac{\Delta}{4}; \quad \text{and}$$

$$f(\frac{\Delta}{2}) = \frac{\Delta}{4}.$$

7. The method according to claim 1, wherein said embedding step (a) produces a value b_i in the said stego signal from a value a_i in said host signal and a value s_i in said message signal, such that said embedding step (a):

(i) is subject to a maximum distortion constraint P,

(ii) employs a continuous periodic function having period Δ, and

(iii) is represented by the function $b_i = E(a_i, s_i)$, and employs an algorithm as follows:

$$\text{if } rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}, \text{ then } p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta}),$$

$$\text{else } p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4};$$

$$e_i = s_i - p_i;$$

$$\text{if } (|\, e_i \,| > \frac{\beta}{2}), \text{ then } e_i = sign(e_i)\frac{\beta}{2};$$

$$q_i = rem(\frac{a_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2}, \text{ then } e_i = -e_i;$$

$$\text{if } a_i > 0, \text{ then } b_i = a_i + e_i;$$

$$\text{else } b_i = a_i - e_i.$$

8. The method according to claim 2, wherein a value b_i in said stego signal is modified after said embedding step (a) to yield a value c_i in said corrupted or distorted stego signal, and wherein said detecting step (b):

(i) produces a value s_{ei} in said estimated message signal from a value c_i in said distorted stego signal,

(ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $s_{ei} = D(c_i)$, and employs an algorithm as follows:

$$q_i = rem(\frac{c_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2}, \text{ then } s_{ei} = 3\frac{\Delta}{4} - q_i,$$

$$\text{else } s_{ei} = q_i - \frac{\Delta}{4}.$$

9. The method according to claim 2, wherein

said host signal is a sequence a_i, for $i = 1$ to N;

said message signal is a sequence s_i, for $i = 1$ to N;

said stego signal is a sequence b_i, for $i = 1$ to N;

said corrupted or distorted stego signal is a sequence c_i, for $i = 1$ to N; and

said estimated message signal is a sequence s_{ei}, for $i = 1$ to N

10. The method according to claim 1, wherein said embedding step (a):

(i) imposes a limit $\frac{\beta}{2}$ on a magnitude difference between a value b_i in said stego signal that is produced from a value a_i in said host signal;

(ii) employs a continuous periodic function having a period Δ to produce said stego signal, wherein such said limit $\frac{\beta}{2}$ and said period Δ are chosen to minimize a mean square distance between said message signal and said estimated message signal, subject to a maximum distortion constraint P of said embedding step (a).

11. A method for mapping K information bits to a message signal s_i, $i = 1$ to N, said method comprising the steps of:

grouping said K information bits together to represent one of 2^L symbols, wherein each said 2^L symbol is mapped to a basis vector or its negative of a $2^{L-1} \times 2^{L-1}$ orthogonal transform matrix.

12. The method according to claim 11, wherein said orthogonal transform matrix is obtained from a cyclic all-pass filter and its ciruclar shifts.

13. The method according to claim 12, wherein said cyclic all-pass filter is obtained from a key.

FIGURE 1

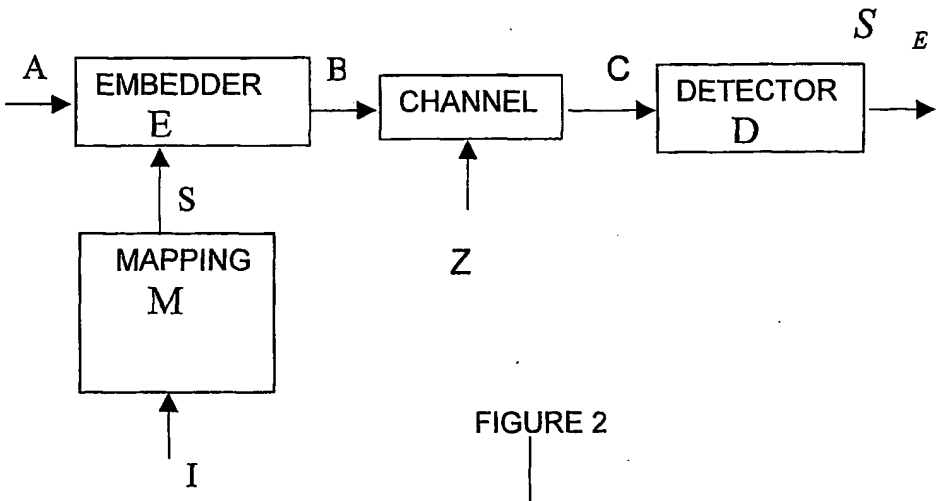


FIGURE 2

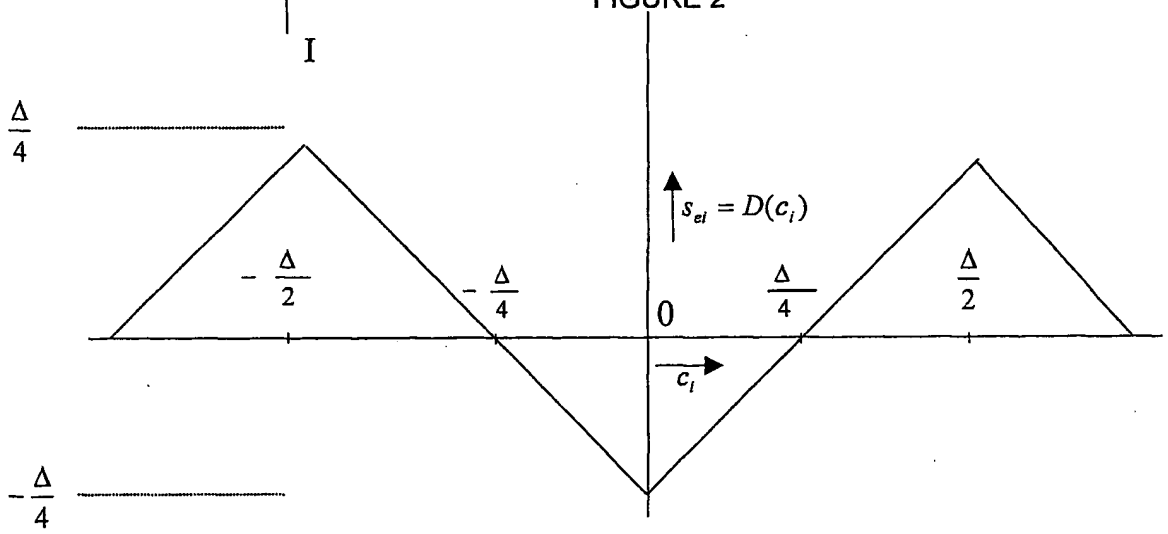
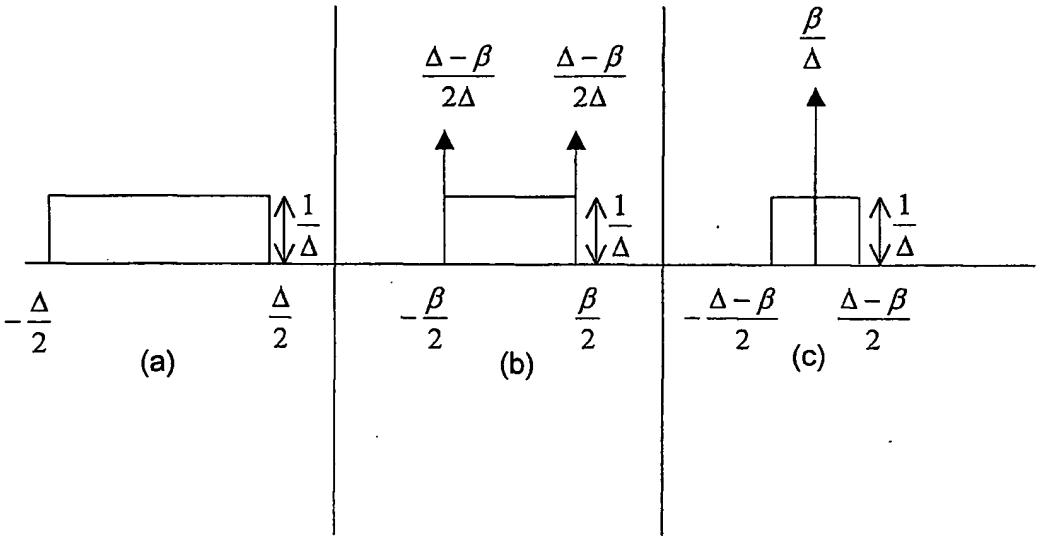


FIGURE 3


$\frac{\beta}{\Delta}$
$\frac{\Delta-\beta}{2\Delta}$
$\frac{\Delta-\beta}{2\Delta}$
$\frac{1}{\Delta}$
$\frac{1}{\Delta}$
$\frac{1}{\Delta}$
$-\frac{\Delta}{2}$
$\frac{\Delta}{2}$
$-\frac{\beta}{2}$
$\frac{\beta}{2}$
$-\frac{\Delta-\beta}{2}$
$\frac{\Delta-\beta}{2}$
(a)
(b)
(c)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24468

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04K 1/02
US CL : 380/252, 253, 254

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/252, 253, 254

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Handbook of Applied Cryptography, Menezes, et. al. CRC Press1997

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, Crypto Proceedings, West, EIC search, STN, Dialog

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,940,135 A (PETROVIC et. al.) 17 August 1999 Figure 3, Columns 2-6	1-13
Y	US 6175627 B1 (PETROVIC et. al.) 16 January 2001Columns 2--6	1-13
Y	US 3897591 A (LUNDSTROM et. al.) 29 July 1975	1-13
Y	US 3427399 A (EHRAT) 11 February 1969	1-13
Y	US 3133991 A (GUANELLA) 19 May 1964	1-13
Y	US 2836657 A (BARTELINK) 27 May 1958	1-13
Y	US 2426225 A (KRAUSE) 26 August 1947	1-13

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 SEPTEMBER 2001	09 JAN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GAIL HAYES Telephone No. (703) 308-4562

Form PCT/ISA/210 (second sheet) (July 1998)★